JOHN DOE (24.5.180.56)

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

PACIFIC CENTURY INTERNATIONAL LTD.,

Plaintiff v.

DOES 1-129, Defendants

Case No. C11-03681 HRL

MOTION TO QUASH ORDER GRANTING PLAINTIFF'S APPLICATION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f)

I, John Doe (24.5.180.56), file a motion to quash the order granting PACIFIC CENTRY INTERNATIONAL LTD. application for leave to take discovery. A copy of this motion will be provided to both the Court and the Plaintiff. The case against DOES 1-129 is a court sanctioned blackmail and extortion campaign to force innocent people to settle out of court for exorbitant amounts to avoid embarrassment about the association with this company and its lawyers. This case should be dismissed immediately based on the following statements:

1) Improper Joinder of Parties.

The claims against me qualify as a unique case. DOES 1-129 all have completely different network configurations both at the Internet Service Provider (ISP) and own person home network level. Each individual DOE deserves a right to an individual investigation with individual accusal and defense. Joinder requires that each case share sufficient overlap to be grouped together. In this case, each DOE relies on entirely separate network configurations, computer and network hardware; as a result this case does not qualify. If allowed to proceed, this would be a gross misuse of joinder.

A motion to quash was granted on an identical case in the Northern District of California, filed by Mr Steele's firm. On August 23, 2011, Judge Joseph C. Spero of the United States District Court for the Northern District of California issued an order severing all but one of the subpoenas. In his order he stated,

"Several judges in the Northern District of California have recently found that use of BitTorrent, like earlier P2P technologies, is not sufficient to satisfy the requirements of Rule 20(a), even if the Doe defendants are part of a single swarm. For the reasons stated below, the Court Finds that the latter approach is more persuasive. Therefore, the Court concludes that permissive joinder of the Doe Defendants is improper under Rule 20(a)." (See Hard Drive Productions v. Does 1-188, case3:2011cv01566 (severed Does 2-188)

On this basis alone, this subpoena should be quashed.

2) Unreliability of IP Address Tracing.

The Plaintiff claims it has produced software that can reliably trace an IP address to a person. I believe that the plaintiff has perjured themselves with this statement as it is completely false. IP-tracing software has repeatedly been proven to be less than 100% reliable. A study conducted by Microsoft Research stated, *"We show that, even without built-in host identities, using IP addresses, anonymized user IDs, and their associated events, we can track a large percentage of host activities with high accuracy. Overall, 76% of the events in the application log can be attributed to hosts, and 92% of hosts can be tracked correctly. This result is consistent across many IP-addressranges [sic], suggesting that tracking host-IP bindings is widely applicable."* This report is freely available at the following URL, http://research.microsoft.com/pubs/80964/sigcomm09.pdf. The software referenced in the complaint, claims that they have 100% reliably in IP address tracing. I find it hard to believe that the Plaintiff has a more reliable software solution than Microsoft who spends millions of dollars in research to solve this problem.

There is also a separate issue here as well. In the case of someone using an unsecured wireless router, an outside party can access their internet connection. This party can surf the internet, send email, upload files, or download content. This unknown outside party would have the same IP Address as anyone on the router itself. Therefore, there is no way to know, reliably and accurately, who the offending party was.

Many courts across the country have ruled against cases for these exact reasons. These cases are too numerous to list here. I ask that the Court support these rulings.

A search on Google reveals dozens of software solutions that allow users to "spoof" or impersonate false IP addresses via a proxy server (intermediary), which are designed to re-reroute traffic and obscure the source as well as the destination. This completely disproves the plaintiff's claim (again) that they are able to 100% pinpoint an individual based upon their IP address.

Common public examples are:
http://www.torproject.org/
http://proxy.org/cgi_proxies.shtml
http://tech-faq.com/proxy

3) Unreliability of MAC Address Tracing.

For the subset of IP addresses that the Plaintiff has successfully tracked, one would need the Media Access Control (MAC address) to find the material that the DOES are accused of downloading. The MAC address would be a unique identifier to a device that downloaded the material. Any device with an internet connection has a unique MAC address. This would include routers, hubs, switches, wireless access points, desktops, laptops, smart phones, network attached storage, etc.

The issue here is that ISPs typically 'bind' to one MAC address. This MAC address would be associated with what is directly connected to the ISPs' modem, which generates the internet connection. In my particular network configuration, the MAC address that my ISP would report would be my wireless router. This device, unless equipped with a storage device, would have no files on it other than the routing software provided by the original equipment manufacturer (OEM). Once again, the Plaintiff has grossly misrepresented their capabilities of tracing. In my network configuration, I have many devices connected to the router, including potential unknown parties connecting through my wireless connection. Any of these could be associated with the complaint. This proves that the Plaintiff's ability to 100% identify a *person* by their MAC address tracing software is completely false.

In addition, there are many solutions (and how-to guides) that are available free and online that allow an individual to impersonate or falsify a MAC addresses (just like IP Addresses). One such example can be found at: http://hidemymacaddress.com/. This makes it extraordinarily difficult to pinpoint a specific device where the alleged offense occurred. The investigation would not know where to look to find the alleged download. This would be especially true if an unknown party connected to my wireless router and will not connect to it again. With this uncertainty, the Plaintiff's investigation would be unable to verify who and where the material was downloaded. As a result, the Plaintiff cannot pledge without a shadow of doubt that I am the one who has alleged downloaded their material.

4) Unreliability of Home Network Security

There is no way for the Plaintiff to prove that the DOES in this complaint had a secured home network during the time of the alleged download. Even in the event that a DOE does have a secured home network, there are numerous ways to circumvent that security. One main example is WEP security, which is considered the lowest wireless security level, as well as the easiest to crack. One website claims that you have the ability to crack a WEP security key in 60 seconds which can be found here: http://www.shawnhogan.com/2006/08/how-to-crack-128-bit-wireless-networks.html.

Another website shows you every single step necessary as well as the appropriate items to buy and the tools to use to make it easier to attack someone's security: http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack

Until very recently, I have used WEP security to secure my wireless network. After reading articles like these, I have changed my security to something more robust. However, with that said, there could have been an unknown party who cracked my WEP security and downloaded the alleged material. Unfortunately, I would have no way of tracking back to this event as there are no log files for me to investigate.

5) Inability to Pinpoint a Person by IP Address

Unfortunately for the Plaintiff, the claim that their ability to Pinpoint a person directly by an IP address is impossible as stated previously. They seem to forget that people share computers within a household. There are several people who use my personal desktop on a regular basis. These people are friends, and family members. Any of these people had the potential of downloading anything they wish. This could have included the alleged content as provided in the complaint.

In the event that someone breeched my wireless security, it would be someone who does not reside in my residence. I live in an area where there are many residences close by to my own. I would have no way of knowing who intercepted my wireless signal and used it for their own nefarious purposes. More so, an unknown party could have been on a laptop in a car across the street accessing my wireless network. There would be no way of knowing. As a result, the Plaintiff has a very difficult job of identifying someone without any doubt.

6) Improper reference to Copyrighted Material

It's my understanding that in order to copyright an idea, work, etc; it must be filed with and registered with the US Copyright Office. The formal complaint that I reviewed includes no reference to a Copyright Number or official document stamped from the US Copyright Office.

According to US Copyright law, materials have to be registered at least three months prior to any infringement in order to pursue statutory damages. As a result, it's unclear if the Plaintiff has any right to pursue this case going forward without official documentation of their copyright.

7) Continued Harassment of Defendants after Cases Dismissed

Mr. Steele and his organization have a tainted record of ignoring the rulings of courts in numerous states. There have been reports of Mr. Steele and his organization continuing to harass and attempt to extort money out of DOES whose cases was dismissed by the judge. Below are some examples of people actively being pursued by Mr. Steele and his organization posted to reddit.com:

edit #5: Got a request to settle from John Steele. I almost lolled because the mac address they listed well...it's not my computer, or routers, or any of my roommates. So...talking to a lawyer real soon about how this dude is trying to extort money from a college student who couldn't pay for his semester of college because of possible legal finances.

I classmate of mine received one of these notices and he was freaking out but the whole thing seems really shady. He contacted the people and the lawyer said that they wanted to take him to court for $250,000 but were willing to settle for $3,000. Of course they sent him documents asking for his bank account and routing number. Of course he doesn't have any money and claims he didn't download a movie. (They won't even tell him what movie they claim he downloaded) This whole thing seems pretty [expletive deleted] shady to me.

In addition, this does not include people who settled out of court before their case was dismissed. I find it appalling that this type of behavior is acceptable in this country. People are being blackmailed for fear of being exposed as avid watchers of pornography. Not to mention exposure of their true sexual orientation in the event that the pornography is homosexual in nature (as some complaints I have found online happened to be). I feel that this is a right to privacy issue that the Plaintiff is completely ignoring and using the Courts at his disposable to step on them.

Conclusion

In conclusion, I motion to quash the subpoena immediately. I find it absolutely astounded that the court has allowed this type of behavior to move forward as far as it has. John Steel and his tactics are questionable at best. I have not, to this day, received a formal complaint regarding this case. I had to go online and purchase (on a fee basis) a copy of the complaint to understand why I received this notice in the mail in the first place. After I reviewed the complaint, I went onto Google and began searching about Mr. Steele and his organization. I have seen numerous posting about complaints of their behavior and

use of intimidation to force a settlement out of honest hardworking Americans. This blackmail campaign is absolutely unacceptable.

My hope is that the court will see through Mr. Steele and his deceptive practices and dismiss this case for what it is truly for, extortion and use of embarrassment to be associated with the porn industry. This is a shakedown at best with a resemblance to the mob. I feel as if I'm being forced to pay a settlement or else my reputation will be tainted with the association with this alleged offense. It is my understanding that some individuals were coerced into paying thousands of dollars for something that could have been purchased for $20 or less online or through a subscription.

For all the reasons outlined previously, I would also ask that the court lecture Mr. Steele and his organization about wasting taxpayer money, the court's time, my time, and causing irreparable mental anguish over these baseless claims. I move that the subpoenas for all DOES including myself be quashed immediately and this case be dismissed.

Dated: 9/30/2011

Respectfully,

s/John Doe
John Doe (24.5.180.56)